THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISIOIN

TRAVIS JAMES, individually and on behalf of all others similarly situated, Plaintiff, v. DAVACO, INC., DAVACO LP, and CRANE WORLDWIDE LOGISTICS LLC, Defendants	Civil Action No.: **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff Travis James ("Plaintiff") brings this Class Action Complaint against Davaco, Inc., Davaco LP, and Crane Worldwide Logistics LLC (collectively, "Defendants"), in his individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard personally identifiable information that Defendants required from their employees as a condition of employment, including without limitation, names, Social Security numbers, and driver's license numbers or government-issued identification numbers (collectively, "personally identifiable information," "Private Information," or "PII"). "Davaco confirmed that the data viewed or taken by the attacker included employees' personal information."[1]

[1] *See Notice of Data Security Incident, available at:* https://www.doj.nh.gov/consumer/security-breaches/documents/davaco-20210716.pdf, a true and correct copy of which is attached hereto as Exhibit 1 ("Ex. 1").

2. Plaintiff also alleges Defendants failed to provide timely, accurate, and adequate notice to Plaintiff and similarly situated current and former employees ("Class Members") that their PII had been lost and precisely what type of information was unencrypted and is now in the possession of unknown third parties.

3. Defendants Davaco, Inc. and Davaco LP (together "Davaco") comprise a multi-site project management and resource deployment firm that supports retail, restaurant, and hospitality services with the development, transformation, and maintenance of their physical sites. Davaco's employees entrust them with an extensive amount of their PII. Davaco retains this information on computer hardware—even after the employment relationship ends. Davaco asserts that they take the privacy and security of such information "very seriously." Ex. 1 at 3.

4. On or before June 11, 2021, Defendants learned of "suspicious activity" on Davaco's computer network. *Id.* at 1. Based on the findings of investigators retained by Defendants, they determined that the suspicious activity on their network involved a ransomware attack on or before June 11, 2021, whereby an unauthorized individual gained access to their network (the "Data Breach"). By June 15, 2021, Defendants had confirmed that in the Data Breach, the attacker viewed and removed data stored in the system, including PII. These servers contained files that in turn contained information about current and former employees, including Plaintiff.

5. Nearly a month later, Defendants issued a "Notice of Data Security Incident," dated July 2, 2021, to those whose PII may have been impacted.

6. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendants admit that the unencrypted PII that the attacker viewed and took included individuals' names, Social Security

numbers, driver's licenses, and/or government issued identification numbers.

7. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. The exposed PII of Plaintiff and Class Members can be sold on the dark web. Plaintiff and Class Members now face a present and lifetime risk of identity theft, which is heightened here by the loss of Social Security and driver's license numbers.

8. This PII was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiff and Class Members. In addition to Defendants' failure to prevent the Data Breach, after discovering the breach, Defendants waited a month to report it to the states' Attorneys General and affected individuals. Defendants have also purposefully maintained in secret the specific vulnerabilities and root causes of the breach and have not informed Plaintiff and Class Members of that information.

9. As a result of this delayed response, Plaintiff and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

10. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal and state statutes.

11. Plaintiff and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses

associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

12. Defendants disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

13. Plaintiff Travis James is a resident and citizen of Pennsylvania. Plaintiff James is acting on his own behalf and on behalf of others similarly situated. Defendants obtained and continue to maintain Plaintiff James' PII and have a legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff James would not have entrusted his PII to Defendants had he known that they would fail to maintain adequate data security. Plaintiff James' PII was compromised and disclosed as a result of the Data Breach.

14. Defendant Davaco, Inc. was founded in 1990, and is a corporation organized under the laws of the State of Texas, with U.S. operations headquartered in the Dallas-Fort Worth Metroplex.

15. Defendant Davaco LP is a limited partnership organized under the laws of Delaware and located at 4050 Valley View Lane, Irving, Texas.

16. Defendant Crane Worldwide Logistics LLC ("Crane") was formed in 2008 as a global provider of customized logistics solutions. Crane is a corporation organized under the laws of the State of Delaware, and is headquartered in Houston, Texas. In 2017, Crane merged with Davaco, Inc.

17. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

18. All of Plaintiff's claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

19. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed Class, and at least one Class Member is a citizen of a state different from Defendants to establish minimal diversity.

20. The Northern District of Texas has personal jurisdiction over Defendants named in this action because Defendants and/or their parents or affiliates are headquartered in this District

and Defendants conduct substantial business in Texas and this District through their headquarters, offices, parents, and affiliates.

21. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendants and/or their parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

22. Defendants are a leading provider of customized logistics solutions. Davaco specifically provides support to clients with multi-site project management and resource deployment for the development, transformation, and maintenance of physical sites, and employs over 1,700 employees across North America.[2]

23. Plaintiff and Class Members employed by Defendants were required to provide Defendants sensitive and confidential information, including their names, dates of birth, Social Security numbers, driver's license or other government issued identification numbers, and other PII, which is static, does not change, and can be used to commit myriad financial crimes.

24. Plaintiff and Class Members, as current and former employees, relied on these sophisticated Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

25. Defendants had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties.

---

2 *See* https://www.davaco.com/about (last visited Sept. 24, 2021).

The Data Breach

26. Beginning on or about July 2, 2021, Defendants sent Plaintiff and other current and former employees a *Notice of Data Security Incident*. Defendants informed the recipients of the notice that:

> **What Happened?**
>
> On June 11, 2021, Davaco was alerted to suspicious activity on our computer network. We hired cybersecurity experts and computer forensic investigators to help us investigate the incident, ensure the safety of our environment, and confirm whether anyone's personal information was impacted. While the investigation is ongoing, we can confirm that we were the victim of a ransomware attack, and an unauthorized individual gained access to our network. Based on the investigation, the attacker viewed and removed some data stored in the system. On June 15, 2021, we confirmed that the data viewed or taken by the attacker included employees' personal information.
>
> **What Information Was Involved?**
>
> The potentially impacted information includes your name, Social Security number, and Driver's license or government issued identification number.[3]

27. On or about July 16, 2021, Defendants sent data breach notifications to various state Attorneys General, including New Hampshire's Attorney General, signed by Lindsay B. Nickle, of Lewis Brisbois Bisgaard & Smith LLP, as counsel for Defendant Davaco LP.[4]

28. Defendants admitted in the *Notice of Data Breach* and the letters to the Attorneys General that unauthorized third persons accessed files that contained sensitive information about Defendants' current and former employees, including individuals' names, Social Security

---

[3] *See* Ex. 1 at 3. Davaco's notice to the New Hampshire Attorney General added: "The investigation has confirmed Davaco was the victim of a ransomware attack and an unauthorized individual gained access to Davaco's network, viewed, and exfiltrated some data stored in the system. On June 15, 2021, Davaco confirmed that the data viewed or taken by the attacker included employees' personal information." *Id.* at 1.

[4] *See* https://www.doj.nh.gov/consumer/security-breaches/documents/davaco-20210716.pdf (last visited Sept. 24, 2021)

numbers, and driver's license numbers or government-issued identification numbers.

29. In response to the Data Breach, Defendants claim that they "retained cybersecurity experts and computer forensic investigators to help investigate the incident, ensure the safety of the environment, and confirm whether any individual's Personal Information was impacted."[5] In addition, Defendants maintain that:

> Davaco is taking steps to prevent a similar event from occurring in the future and to protect the privacy and security of all sensitive information in its possession. These steps include upgrading its email environment and implementing multi-factor authentication for accounts in the environment, implementation of Palo Alto anti-phishing and security measures, and the deployment of endpoint protection to devices in the Davaco network.[6]

However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

30. The unencrypted PII of Plaintiff and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

31. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of PII for 14,578 current and former employees.[7]

---

5 *Id.* at 1.

6 *Id.* at 2.

7 *See* State of Maine Data Breach Notification Information, *available at*: https://apps.web.maine.gov/online/aeviewer/ME/40/07bf9dbb-2a4a-47d4-9530-1a0d446b5c6c.shtml (last visited Sept. 24, 2021).

32. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[8]

33. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

---

[8] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Sept. 24, 2021).

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[9]

34. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)....

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it....

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any

---

9 *Id.* at 3-4.

links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic....[10]

35. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

---

[10] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at:* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Sept. 24, 2021).

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[11]

36. Given that Defendants were storing the PII of tens of thousands of current and former employees, Defendants could and should have implemented all of the above measures to prevent and detect ransomware attacks.

37. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of thousands of current and former employees, including Plaintiff and Class Members.

Defendants Acquire, Collect, and Store the PII of Plaintiff and Class Members.

38. Defendants have historically acquired, collected, and stored the PII of Plaintiff and Class Members.

39. As a condition of maintaining employment with Defendants, Defendants require that their employees entrust them with highly confidential PII.

40. By obtaining, collecting, and storing the PII of Plaintiff and Class Members,

---

[11] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Sept. 28, 2021).

Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

41. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

42. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members. Alternatively, Defendants could have destroyed the data, especially decade-old data from former employees.

43. Defendants' policies on their website include promises and legal obligations to maintain and protect PII, demonstrating an understanding of the importance of securing PII. For example, Davaco's Privacy Statement provides in part:

> **Security** –
>
> DAVACO uses industry-standard efforts to safeguard the confidentiality of your personal information such as firewalls and authentication protection.[12]

44. Davaco, Inc.'s Privacy Statement further assures that it has a "firm commitment" to privacy and that "[t]he success of our business depends upon our ability to maintain the trust of our users."[13]

45. Defendants' negligence in safeguarding the PII of Plaintiff and Class Members is

---

12 *See* https://www.davaco.com/legal (last visited Sept. 24, 2021).

13 *Id.*

exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

46. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

47. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[14] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[15]

48. The ramifications of Defendants' failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personally Identifiable Information

49. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, Personal Information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[16] Experian reports that a stolen credit or debit

---

14 17 C.F.R. § 248.201 (2013).

15 *Id.*

16 *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Sept. 24, 2021).

card number can sell for $5 to $110 on the dark web.[17] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[18]

50. Social Security numbers, for example, are among the worst kind of Personal Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[19]

51. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

52. Even then, a new Social Security number may not be effective. According to Julie

---

[17] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Sept. 24, 2021).

[18] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Sept. 24, 2021).

[19] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Sept. 24, 2021).

Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[20]

53. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license number or government-issued identification number, name, and date of birth.

54. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[21]

55. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

56. The fraudulent activity resulting from the Data Breach may not come to light for years.

57. There may be a time lag between when harm occurs versus when it is discovered,

---

[20] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Sept. 24, 2021).

[21] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Sept. 24, 2021).

and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[22]

58. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers and dates of birth, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

59. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

60. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' file servers, amounting to potentially tens or hundreds of thousands of individuals' detailed, Personal Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

61. In the breach notification letter, Defendants made an offer of 12-months of identity monitoring services to its members that had their Social Security numbers breached; but did not offer this to those whose other information was subject to the Data Breach. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of

---

[22] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Sept. 24, 2021).

data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, medical and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

62. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Plaintiff Travis James' Experience

63. Plaintiff James was required to provide his PII to Davaco in connection with his employment at Davaco in or about 2015.

64. In or around July 2021, Plaintiff James received notice from Davaco that his PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff James' PII, including name and one or more of his Social Security number, and driver's license number or government-issued identification number, was compromised as a result of the Data Breach.

65. As a result of the Data Breach, Plaintiff James made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; researching and signing up for credit monitoring and identity theft protection services offered by Davaco; researching, signing up for, and paying approximately $20 per month for credit monitoring and identity theft protection services from LifeLock; placing a freeze on his credit with all three bureaus; and contacting creditors and credit bureaus regarding numerous fraudulent attempts by unauthorized third parties to use his name and Social Security number to obtain residential rental contracts. Plaintiff James

has spent at least five hours dealing with the Data Breach, valuable time Plaintiff James otherwise would have spent on other activities, including but not limited to work and/or recreation.

66. As a result of the Data Breach, multiple unauthorized third parties attempted to use Plaintiff James' name and Social Security number to secure rental contracts for apartments. Each attempt, beginning on or about August 26, 2021 and continuing through on or about September 6, 2021, caused various credit bureaus to conduct a "hard pull" on Plaintiff James' credit reports. As a result, Plaintiff James' credit score was materially and negatively impacted and has yet to recover to its pre-August 26, 2021 level.

67. As a result of the Data Breach, Plaintiff James has suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff James is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

68. Plaintiff James suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Davaco obtained from Plaintiff James; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

69. As a result of the Data Breach, Plaintiff James anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff James will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ALLEGATIONS

70. Plaintiff brings this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

71. The Class that Plaintiff seeks to represent is defined as follows:

> All individuals residing in the United States whose PII was compromised in the data breach first announced by Defendants on or about July 2, 2021 (the "Class").

72. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

73. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

74. Numerosity, Fed R. Civ. P. 23(a)(1): The Class is so numerous that joinder of all members is impracticable. Defendants have identified 14,578 individuals whose PII may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendants' records.

75. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendants had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendants had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendants had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII of Plaintiff and Class Members;

e. Whether and when Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendants' wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the

imminent and currently ongoing harm faced as a result of the Data Breach.

76. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because he had his PII compromised as a result of the Data Breach due to Defendants' misfeasance.

77. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

78. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

79. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary

duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

80. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

81. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

82. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

83. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII of Class Members, Defendants may continue to refuse to provide proper

notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Amended Complaint.

84. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

85. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendants breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendants on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendants breached the implied contract;

f. Whether Defendants adequately, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information

compromised in the Data Breach;

h. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and,

i. Whether Class Members are entitled to actual damages, statutory damages, nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

COUNT I

NEGLIGENCE

86. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 85.

87. As a condition of their employment with Defendants, Defendants' current and former employees were obligated to provide Defendants with certain PII, including their names, Social Security numbers, and driver's license numbers or government-issued identification numbers.

88. Plaintiff and the Class entrusted their PII to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

89. Defendants have full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

90. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

91. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that the PII of Plaintiff and the Class in Defendants' possession was adequately secured and protected.

92. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former employees' PII, and that of their beneficiaries and dependents, they were no longer required to retain pursuant to regulations.

93. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Class.

94. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendants with their confidential PII, a necessary part of employment with the company.

95. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff or the Class.

96. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

97. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendants' systems.

98. Defendants' own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and the Class, including basic encryption techniques freely available to Defendants.

99. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendants' possession.

100. Defendants were in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

101. Defendants had and continue to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

102. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class.

103. Defendants have admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

104. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Class during the time the PII was within Defendants' possession or control.

105. Defendants improperly and inadequately safeguarded the PII of Plaintiff and the

Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

106. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Class in the face of increased risk of theft.

107. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of their current and former employees' PII, and that of their beneficiaries and dependents.

108. Defendants breached their duty to exercise appropriate clearinghouse practices by failing to remove former employees' PII, and that of their beneficiaries and dependents, they were no longer required to retain pursuant to regulations.

109. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

110. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

111. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

112. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by

businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

113. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

114. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

115. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

116. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

117. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and

identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

118. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

119. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

120. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT II

BREACH OF IMPLIED CONTRACT

121. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 85.

122. Defendants required Plaintiff and the Class to provide their Personal Information, including names, addresses, Social Security numbers, driver's license numbers or government issued identification numbers, and other Personal Information, as a condition of their employment.

123. As a condition of their employment with Defendants, Plaintiff and the Class provided their Personal Information. In so doing, Plaintiff and the Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

124. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendants.

125. Defendants breached the implied contracts they made with Plaintiff and the Class by failing to safeguard and protect their Personal Information, and by failing to provide timely and accurate notice to them that Personal Information was compromised as a result of the Data Breach.

126. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT III

INVASION OF PRIVACY

127. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 85.

128. Plaintiff and the Class had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

129. Defendants owed a duty to their current and former employees and their beneficiaries and dependents, including Plaintiff and the Class, to keep their PII contained as a part thereof, confidential.

130. Defendants failed to protect and released to unknown and unauthorized third parties the PII of Plaintiff and the Class.

131. Defendants allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and the Class, by way of Defendants' failure to protect the PII.

132. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and the Class is highly offensive to a reasonable person.

133. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Class disclosed their PII to Defendants as part of the current and former employees' employment with Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

134. The Data Breach at the hands of Defendants constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their persons or as to

their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

135. Defendants acted with a knowing state of mind when they permitted the Data Breach to occur because they were with actual knowledge that their information security practices were inadequate and insufficient.

136. Because Defendants acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class.

137. As a proximate result of the above acts and omissions of Defendants, the PII of Plaintiff and the Class was disclosed to third parties without authorization, causing Plaintiff and the Class to suffer damages.

138. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class in that the PII maintained by Defendants can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

COUNT IV

BREACH OF CONFIDENCE

139. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 85.

140. At all times during Plaintiff's and the Class's interactions with Defendants, Defendants were fully aware of the confidential and sensitive nature of Plaintiff's and the Class's PII that Plaintiff and the Class employed by Defendants provided to Defendants.

141. As alleged herein and above, Defendants' relationship with Plaintiff and the Class was governed by terms and expectations that Plaintiff's and the Class's PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

142. Plaintiff and the Class employed by Defendants provided Plaintiff's and the Class's PII to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the PII to be disseminated to any unauthorized third parties.

143. Plaintiff and the Class employed by Defendants also provided Plaintiff's and the Class's PII to Defendants with the explicit and implicit understandings that Defendants would take precautions to protect that PII from unauthorized disclosure.

144. Defendants voluntarily received in confidence Plaintiff's and the Class's PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

145. Due to Defendants' failure to prevent and avoid the Data Breach from occurring, Plaintiff's and the Class's PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and the Class's confidence, and without their express permission.

146. As a direct and proximate cause of Defendants' actions and/or omissions, Plaintiff and the Class have suffered damages.

147. But for Defendants' disclosure of Plaintiff's and the Class's PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' Data Breach was the direct and legal cause of the theft of Plaintiff's and the Class's PII as well as the resulting damages.

148. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiff's and the Class's PII. Defendants knew

or should have known their methods of accepting and securing Plaintiff's and the Class's PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and the Class's PII.

149. As a direct and proximate result of Defendants' breach of their confidence with Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of current and former employees and their beneficiaries and dependents; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

150. As a direct and proximate result of Defendants' breaches of confidence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT V

UNJUST ENRICHMENT

151. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 85.

152. Defendants benefited from receiving Plaintiff's and Class Members' PII by their ability to retain and use that information for their own benefit. Defendants understood this benefit.

153. Defendants also understood and appreciated that Plaintiff's and Class Members' PII was private and confidential, and its value depended upon Defendants maintaining the privacy and confidentiality of that PII.

154. Plaintiff and Class Members conferred a monetary benefit upon Defendants in the form of their employment, and in connection thereto, by providing their PII to Defendants with the understanding that Defendants would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, they were required to provide Defendants with their PII. In exchange, Plaintiff and Class members should have received adequate protection and data security for such PII held by Defendants.

155. Defendants knew Plaintiff and Class members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

156. Defendants failed to provide reasonable security, safeguards, and protections to the PII of Plaintiff and Class Members.

157. Under the principles of equity and good conscience, Defendants should not be permitted to retain money belonging to Plaintiff and Class members, because Defendants failed to implement appropriate data management and security measures mandated by industry standards.

158. Defendants wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

159. Defendants' enrichment at the expense of Plaintiff and Class Members is and was unjust.

160. As a result of Defendants' wrongful conduct, as alleged above, Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendants, plus attorneys' fees, costs, and interest thereon.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, request judgment against Defendants and that the Court grant the following:

A. For an Order certifying the Class, as defined herein, and appointing Plaintiff and his Counsel to represent each such Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable

regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendants from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing

checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third

parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: September 29, 2021

Respectfully Submitted,

BALON B. BRADLEY
BALON B. BRADLEY LAW FIRM
Texas Bar No. 02821700
11910 Greenville Ave., Suite 220
Dallas, TX 75243
Telephone: 972-991-1582
Facsimile: 972-755-0424
balon@bbradleylaw.com

RACHELE R. BYRD
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: (619) 239-4599
Facsimile: (619) 234-4599
byrd@whafh.com

M. Anderson Berry
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com

Attorneys for Plaintiff and the Proposed Class

Exhibit 1

LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Lindsay B. Nickle
2100 Ross Ave, Suite 2000
Dallas, TX 75201
Phone: (214) 722-7141
Mobile: (806) 535-0274
Email: Lindsay.Nickle@lewisbrisbois.com

July 16, 2021

VIA E-MAIL
Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General Knudsen:

We represent Davaco LP ("Davaco") with respect to a recent data security incident described in greater detail below.

1. **Nature of the security incident.**

On June 11, 2021, Davaco was alerted to suspicious activity on its computer network. Davaco retained cybersecurity experts and computer forensic investigators to help investigate the incident, ensure the safety of the environment, and confirm whether any individual's personal information was impacted. The investigation has confirmed Davaco was the victim of a ransomware attack and an unauthorized individual gained access to Davaco's network, viewed, and exfiltrated some data stored in the system. On June 15, 2021, Davaco confirmed that the data viewed or taken by the attacker included employees' personal information. The potentially impacted information includes individuals' names, Social Security numbers, and driver's licenses and/or government issued identification numbers.

2. **Number of New Hampshire residents affected.**

A total of 20 residents of New Hampshire were potentially impacted by this security incident. Notification letters were mailed, via first class mail, to potentially impacted individuals on July 2, 2021. A sample copy of the notification letter is included with this letter.

3. Steps taken relating to the incident.

Davaco is taking steps to prevent a similar event from occurring in the future and to protect the privacy and security of all sensitive information in its possession. These steps include upgrading its email environment and implementing multi-factor authentication for accounts in the environment, implementation of Palo Alto anti-phishing and security measures, and the deployment of endpoint protection to devices in the Davaco network. In addition, the notified individuals have been offered complimentary credit and identity monitoring services through IDX. Davaco has also established a toll-free call center through IDX to answer any questions about the incident and address related concerns. The call center is available Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Standard Time. We have also provided notification to the major credit reporting agencies.

4. Contact Information.

Davaco remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at 214.722.7141 or via email at Lindsay.Nickle@lewisbrisbois.com.

Sincerely,

Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl.: Sample Consumer Notification Letter

To Enroll, Please Call:
833-909-3912
Or Visit:
https://response.idx.us/davaco
Enrollment Code:
<<XXXXXXXX>>

DAVACO
P.O. Box 1907
Suwanee, GA 30024

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

July 2, 2021

Re: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

We are writing to provide you with information about a recent data security incident that may have involved your personal information. At Davaco, we take the privacy and security of our employees' information very seriously. That is why we are sending you this letter to tell you about the incident, offering you credit monitoring and identity monitoring services, and providing you with information, resources and steps you can take to help protect your personal information.

What Happened? On June 11, 2021, Davaco was alerted to suspicious activity on our computer network. We hired cybersecurity experts and computer forensic investigators to help us investigate the incident, ensure the safety of our environment, and confirm whether anyone's personal information was impacted. While the investigation is ongoing, we can confirm that we were the victim of a ransomware attack, and an unauthorized individual gained access to our network. Based on the investigation, the attacker viewed and removed some data stored in the system. On June 15, 2021, we confirmed that the data viewed or taken by the attacker included employees' personal information.

What Information Was Involved? The potentially impacted information includes your name, Social Security number, and Driver's license or government issued identification number.

What We Are Doing. As soon as we discovered the incident, we took the steps described above. We also notified the FBI and will fully cooperate with any law enforcement investigation. In addition, although we have no evidence that your personal information has been misused, we are offering you identity theft protection services through IDX®, the data breach and recovery services expert, these services include: <<12/24>>months of credit monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. If you complete the sign-up steps specified in this letter, the product we are offering you will provide protection from the misuse of any personal information that may have been impacted by this incident.

What You Can Do. We encourage you to contact IDX with any questions and to enroll in the free services we are offering by calling 833-909-3912 or going to https://response.idx.us/davaco and using the Enrollment Code provided above. IDX experts are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is October 2, 2021. It is important to contact IDX with questions. DAVACO has hired IDX as a full-service provider to its employees; as such, DAVACO management does not have details of these services.

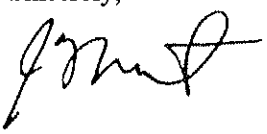
At this time, we are unaware of the misuse of any of your information. However, we encourage you to take full advantage of this service offering. IDX representatives can answer questions or concerns you may have regarding protection of your personal information.

For More Information:

Further information about how to help protect your personal information appears on the following page. If you have questions or need assistance, please call 833-909-3912, Monday through Friday from 9 am - 9 pm Eastern Time.

We take your trust in us and this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,



J. Lamar Roberts, CFO